Our best attempt at fixing the internet

Frederic Jacobs
www.fredericjacobs.com
me@fredericjacobs.com

ABSTRACT

Over the last few months, the Snowden revelations have brought to light the wide-scale surveillance. NIST and other organisations have voluntarily weakened encryption standards on the Internet and have put us all at risk, not only from dragnet surveillance but also from our communications to be hijacked by other people. In addition to that, the security community has for too long ignored from it's threat model attackers that are in control of most nodes of the network. The goal of this paper is to outline the issues of the current model we have for the internet and give a quick overview of how to solve those. Given the 10 pages constraint of this paper, some concepts won't be explained and are considered pre-requisites. If some of them don't sound easy to understand, going to the appendice, might help.

1. INTRODUCTION

1.1 Defining user privacy

Attempt to build a safer internet.

We want it to be compatible with our actual infrastructure and on the machines that are now on the field.

Our threat model assumes that any wire can be tapped. No connection is safe. Source IP spoofing.

2. SCOPE

This paper attempts to fix the confidentiality features of the Internet by introducing a distributed and non-hierarchical domain name system and providing a replacement for TCP at the transport layer.. Meta-data, that can be connected at the IP-level such as the source and destination of a communications will still be collectable. Nevertheless, we think that the suggested enhancements of this paper should help anonymity projects like The Tor Project to speed up substantially their network which is one of their key issues. (Tor project investigates SPEEDY)

3. MOTIVATION

When the Internet was designed at DARPA, the primary goal was to design a system that could provide interconnection between multiple computers. The Web then came by with the motivation to be able to freely exchange information. The Internet has mainly been used for open communications. Any computer on the network could request files. But, over time, people started trusting the internet more and more and with the appearance of services. But the Internet grew so quickly out of what DARPA proposed for a trusted environment. The threat model of the internet changed and our

Introduce current system. Domain name registrars, DNS ...

3.1 Issues with the current system

Zooko's triangle

3.2 How to fix it

3.2.1 *Certificate Pinning*

Works great but not scalable - first fix.

3.2.2 *DANE*

Works great but still having a centralized registry / domain registrars DNSSec

3.2.3 *Tor Hidden Services*

Good, but as seen in Zooko's triangle we don't have the unique address.

3.2.4 *Squaring Zooko's triangle*

Bitcoin chain

4. TRANSPORT SECURITY

What's wrong with tcp is slow and insecure. How to move away from it? Well, we don't really have any other option to base it on UDP. But we love reliability!

Minimalt

Doesn't solve anonimity ==¿ Tor

Issues with too big frames for firewalls?

5. THE *BODY* OF THE PAPER

6. CONCLUSIONS

//

7. ACKNOWLEDGMENTS

This section is optional; it is a location for you to acknowledge grants, funding, editing assistance and what have you. In the present case, for example, the authors would like to thank Gerald Murray of ACM for his help in codifying this *Author's Guide* and the **.cls** and **.tex** files that it describes.

8. ADDITIONAL AUTHORS

9. REFERENCES

9.1 References

APPENDIX

Define Perfect forward secrecy

Using Elliptic curve crypto but not backdoored.

Impact on censorship(when encrypted blobs can be transferred)

A. FINAL THOUGHTS